JOINT ANSSI – ENISA PRESENTATION ON THE ECCG SUB-GROUP ON CRYPTOGRAPHY

Philippe Blot
Cybersecurity Certification Unit
ENISA

Henri Gilbert
Crypto Laboratory
ANSSI, France

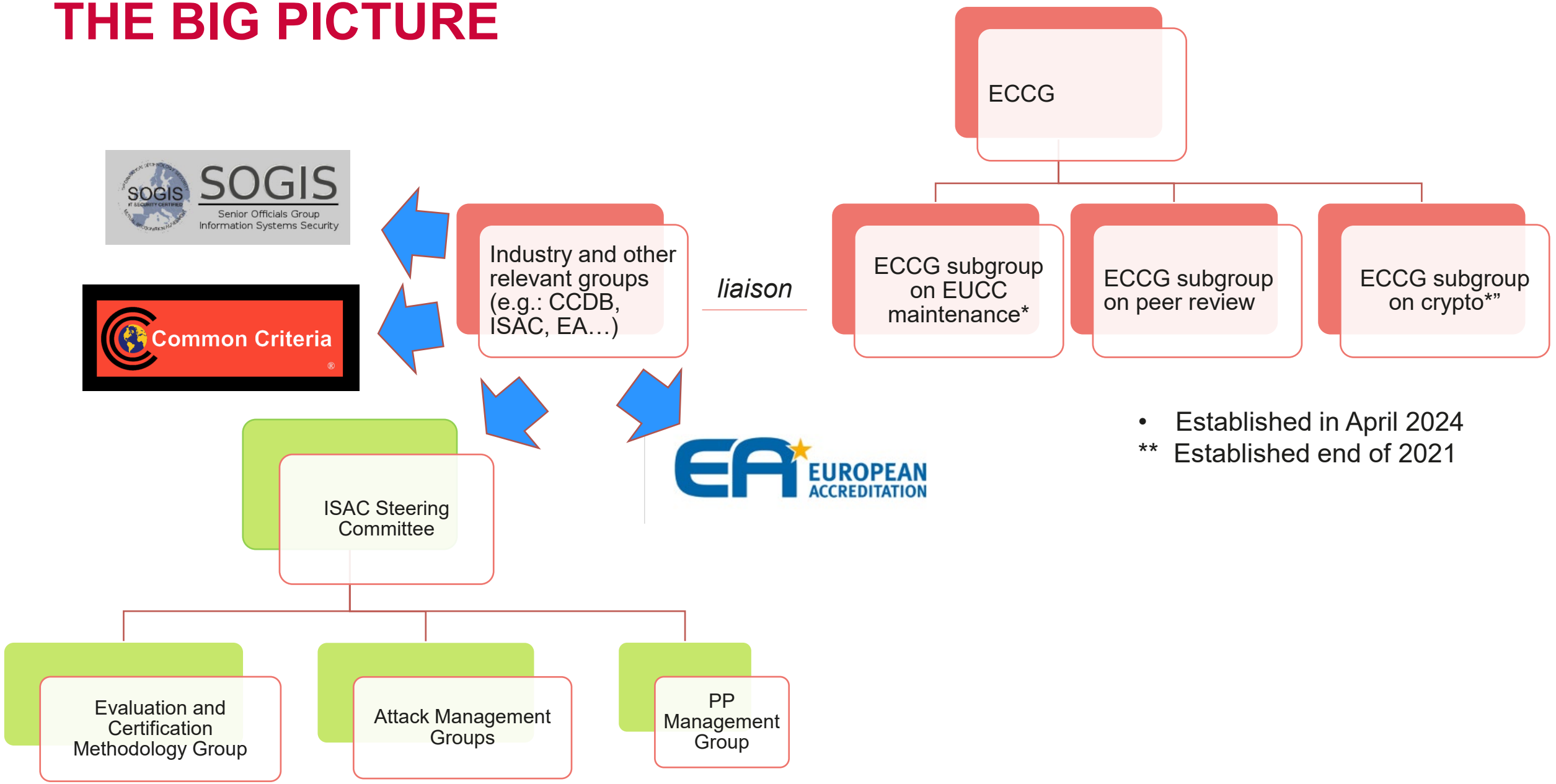
Presentation of the sub-group and its interplay with other groups

A focus on ACM

Other activities

European Conference on PQC Migration, The Hague, 3/12/2025

THE BIG PICTURE



- Established in April 2024

** Established end of 2021

ECCG SUBGROUP ON CRYPTOGRAPHY

Members

- Member States representatives + ENISA + EC
- Representants of 15 MSs attend regularly

2025 activities

- 5 full meetings

Liaisons and interplay

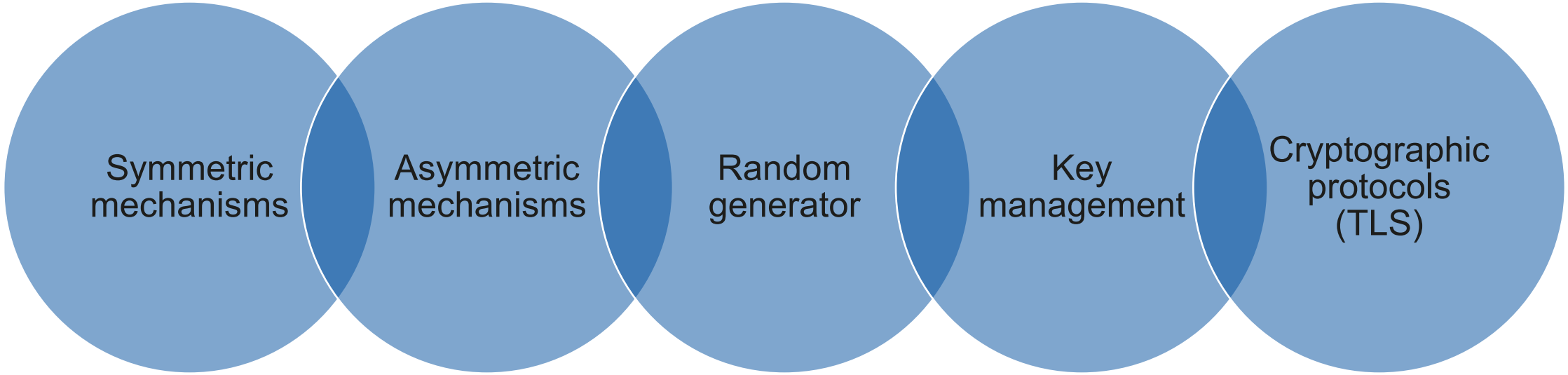
- EU level:
  - SOG-IS crypto subgroup for continuation of their activities
  - NIS2 PQC group for technical support
  - Request from ETSI to continue referencing ACM for eIDAS
- International: CCDB, NIST

AGREED CRYPTOGRAPHIC MECHANISMS

Document developed by SOG-IS crypto group – v1.3 in SOG-IS

The version 2.0 has been adopted under EUCC as guidance document on May 6th:
https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

“White” list of agreed algorithms including recommendations and warnings



AGREED CRYPTOGRAPHIC MECHANISMS V2.0

The main objective of v2.0 is to cover Post-Quantum threat:

- ✓ **Approved PQC schemes are now part of the agreed mechanisms**
- ✓ **Hybridisation is key: Pair post-quantum and classical schemes such that if one breaks, the security remains**

Now let's pass the floor to ANSSI, the editor of ACM

PQC requirements in ECCG crypto guidelines «Agreed Cryptographic Mechanisms » [ACM v2.0]

The ACM « catalogue » in a nutshell

- Aim: serve as guidelines regarding crypto in commercial security products
  - primarily addressed to: developers + **cybersecurity certification** evaluators
  - maintained by: SOG-IS/Crypto until 2024, now by ECCG/Crypto, edited by ANSSI (FR)
  - regular updates: every 2-3 years. Current version: ACM v2.0 (April 2025)

- A white list of ***agreed*** classical and/or post-quantum ***cryptographic mechanisms*** [completed by a comprehensive set of ***caveat notes***]
  - ***agreed*** ≡ mutually recognised by national cybersecurity certification authorities in Europe
  - ***mechanisms*** ≡ symmetric or asymmetric algorithms
    comprise: 1) primitives, 2) constructions (modes or schemes), 3) protocols

- Two types of agreed mechanisms
  - **R** (**recommended**)
    - fully compliant with the state of the art, **security level** * ≥ 125 bits
  - **L** (**legacy**)
    - acceptably robust, though less conservative, **security level** *: typically ≥ 100 bits
    - for such mechanisms, a **validity period** or a **minimum validity period** is specified [by default: ≥ 2031]

(*) security level ≡ time complexity of the best known attack, measured as a number of large operations on a logarithm scale assessed in the classical or quantum computation model depending on the considered context

A small example: block ciphers section of ACM

Agreed Block Ciphers.

Primitive	Parameters' sizes	R/L	Notes
AES [FIPS197, ISO18033-3]	k = 128 bits	R	3-QuantumThreat
	k = 192 bits	R	
	k = 256 bits	R	
Triple-DES [FIPS46-3, ISO18033-3]	k = 168 bits	L[2027]	2-SmallBlocksize 3-QuantumThreat

Note 2-SmallBlocksize. Block ciphers are used in modes of operation to provide a wide variety of security functionalities. In the majority of the cases, the modes fulfill their security objective as long as less than $2^{n/2-5}$ n-bit blocks are processed by the block cipher with a given key. For small block sizes, e.g. 64 bits, and high throughput applications, e.g. securing gigabit network, this may be an issue, e.g., when the key renewal rate is lower than what is required by the data throughput.

Note 3-QuantumThreat. There exist algorithms leveraging quantum computers, like the Grover algorithm, that may speed up attacks against block ciphers. Such attacks may be performed "retroactively": the ciphertext can be stored now and decrypted later when a quantum computer becomes available. In contexts where resistance against attacks leveraging quantum computers is required, it is recommended not to use block ciphers with key size smaller than 192 bits.

PQC requirements in ACM

- Mostly introduced in 2024-25
  - when moving from SOG-IS ACM v1.3 version to ECCG ACM v2.0 version
- General recommendations

  - address the quantum threat asap, using **agreed PQC mechanisms**, at least in the following cases
    - potential vulnerability to retroactive / « harvest now decrypt later » attacks
    - long-lived products

    [for the time being, this is only expressed in incitative, but non-coercitive statements in ACM]

  - roll-out PQC cryptography in **hybrid mode**, by systematically combining:
    - **agreed asymmetric PQC mechanisms**
    - with **agreed asymmetric classical mechanisms** and/or **symmetric keying** (i.e., a pre-shared key)

    [except for hash-based signatures, for which hybridization is optional]

- Extra (milder) recommendation
  - adapt the parameter lengths of agreed symmetric mechanisms, e.g. key and hash lengths

Agreed asymmetric post-quantum mechanisms

- Key establishment

  - 2 agreed post-q **key encapsulation mechanisms (KEMs)** *for the time being*
    - ML-KEM-768 or 1024 [FIPS 203 + ISO 8033-2 Amd 2], i.e. instances with NIST security level III or V
    - Frodo-KEM-976 or 1344 [ISO 8033-2 Amd 2]: while less efficient, might suit some high security applications
  - two agreed **key combiners** for hybridization *for the time being*
    - based on CatKDF [ETSI, IETF draft / Hybrid TLS]
    - based on CasKDF [ETSI, IETF draft / IKEv2]

- Digital signatures

  - 4 agreed post-q **digital signature schemes** *for the time being*
    - ML-DSA-65 or 87 [FIPS 204], i.e. MLWE-based signatures
    - SLH-DSA [FIPS 205], i.e. stateless hash-based signatures
    - XMSS and LMS [SP800-208], i.e. stateful hash-based signatures
  - **composite signatures** for hybridization
    - optional for hash-based signatures
    - can consist of the concatenation of a pre-quantum signature and a post-quantum signature
      [*in contexts where there is no need for a* ***non-separable*** *composite signature*]

Dimensioning of symmetric algorithms in contexts where quantum security is sought

- **Block ciphers**
  - AES-128, AES-192 and AES-256 are all agreed
  - It is recommended to use AES-192 or AES-256 rather than AES-128

Rationale

- The use of AES-128 can be estimated sufficient to thwart quantum attacks based on Grover's algorithm beyond the potential emergence of CRQCs

  Indeed, the speed-up w.r.t. exhaustive search allowed by (parallel) implementations of Grover's algorithm over several circuits is upper bounded by the circuit depth of the computations: this considerably limits this speed-up as compared with the naive 2^{64} factor one would get if ignoring circuit depth limitations.
- The use of AES-192 or 256 allows to ensure: quantum security level > 128 bits

  The achieved security margin is larger, more independent from quantum computation technology considerations, and sufficient to comfortably cover multi-user attacks.

- **Hashing**
  - SHA-2 and SHA-3 instances with hash lengths 256, 384 and 512 bits are all agreed
  - It recommended to use SHA-2 or SHA-3 instances of hash length at least 384 bits

  NB: this does not apply to preimage-resistant hash functions used in agreed standardized hash-based signatures

- **Cryptographic post-processing of random number generators**
  - NIST HMAC-, Hash- and CTR-DRBGs [SP800-90A, ISO18031] are all agreed
  - It is recommended not to use CTR-DRBG with keys smaller than 192 bits

OTHER ACTIVITIES OF THE SUB-GROUP

HEP

- Draft « Harmonised Evaluation Procedure » document developed by SOG-IS
- Built in mirror of ACM with the objective of defining the minimum activities to perform to evaluate the conformity of ACM algorithms
- This document will be updated for consistency with ACM v2.0

PQC and other consutancy

- Support of NIS2 PQC group through review of documents and discussions, and possibly peer review of new mechanims
- Review of Anonymous Credentials from ECDSA, a Google proposal for age verification

Development of testing material

- Conformance testing:
  - Conformance tests developed under SOG-IS, update and verification planned
  - EU implementation of CAVP for conformance testing under discussion with NIST
- Robustness testing: via the ISAC technical groups

HOW TO STAY TUNED?

ENISA dedicated website:

https://certification.enisa.europa.eu/